UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,214	04/18/2001	Peter T. Dinsmore	NAI1P089/00.175.01	6427

28875 7590 11/03/2005	EXAMINER
Zilka-Kotab, PC	LAFORGIA, CHRISTIAN A
P.O. BOX 721120	

	ART UNIT	PAPER NUMBER
SAN JOSE, CA 95172-1120	2131	

DATE MAILED: 11/03/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>03 August 2005</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-21,28-30,38 and 39</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-21,28-30,38 and 39</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   The amendment filed on 03 August 2005 has been noted and made of record.

2.   Claims 1-21, 28-30, 38, and 39 have been presented for examination.

3.   Claims 22-27, 31-37 have been cancelled as per Applicant's request.

Claim Rejections - 35 USC § 102

4.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5.   Claims 1-6, 8-16, and 19-21 are rejected under 35 U.S.C. 102(e) as being anticipated by

U.S. Patent No. 6,941,457 to Gundavelli et al., hereinafter Gundavelli.

6.   As per claim 1, Gundavelli discloses an environment that includes a plurality of users,

wherein each user possess secrets that are shared by respective sets of said plurality of users, a

secret updating method, comprising:

       (a) updating at least one compromised secret known by at least one evicted user using at

least one non-compromised secret that is not known by said at least one evicted user (column 5,

lines 47-63, column 11, lines 6-39).

7.   Regarding claim 2, Gundavelli teaches wherein said updating comprises updating a

plurality of compromised secrets (column 11, lines 6-18, i.e. techniques are applicable in which

members are deleted).

8.   Regarding claim 3, Gundavelli discloses wherein said updating comprises updating all

compromised secrets (column 11, lines 18-25, i.e. remaining members use newly established

secret key).

9.   Regarding claim 4, Gundavelli discloses wherein said updating comprises updating at

least one compromised secret known by one evicted user (column 5, lines 47-63, column 11,

lines 6-39).

10.   With regards to claims 5, 14, and 15, Gundavelli teaches wherein said updating occurs

upon an eviction event, wherein only said second user or the second user and one or more other

users are evicted (column 5, lines 47-63, column 11, lines 6-18, i.e. member departs, members

are deleted).

11.   Regarding claim 6, Gundavelli teaches wherein said updating comprises updating at least

one compromised secret known by a plurality of evicted users (column 11, lines 6-18, i.e.

techniques are applicable in which members are deleted).

12.   Regarding claim 8, Gundavelli teaches wherein said updating comprises updating a

compromised secret using one non-compromised secret (column 5, lines 47-63, column 11, lines

6-39).

13.   Regarding claim 9, Gundavelli teaches wherein said updating comprises updating a compromised secret known by a set of users using a non-compromised secret of a subgroup of said set of users (column 5, lines 47-63, column 11, lines 6-39).

14.   Regarding claim 10, Gundavelli teaches wherein said updating does not use new secret information (column 5, lines 47-63, column 11, lines 6-39).

15.   Regarding claim 11, Gundavelli teaches wherein said compromised secret is shared by said plurality of users (column 5, lines 47-63, column 11, lines 6-39).

16.   Regarding claim 12, Gundavelli teaches wherein said secrets enables secure communication (column 11, lines 15-18, i.e. multicast group can communicate over a secure channel).

17.   As per claim 13, Gundavelli teaches an environment that includes a plurality of users, wherein a first user possesses a set of keys, said set of keys including a first key that enables secure communication among a set of sets, said set of users including at least said first user and a second user, a keying method, comprising:

(a) upon eviction of at least said second user, determining an updated first key using information that includes said first key and a second key, wherein said second key enables secure communication among a subgroup of said set of users, wherein said subgroup does not include

users subject to said eviction (column 5, lines 47-63, column 11, lines 6-39, i.e. forming new group with no evicted users).

18.   Regarding claim 16, Gundavelli teaches wherein said determining uses a function having the following properties:

(1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key (column 5, lines 47-63, column 11, lines 6-39).

19.   Regarding claim 19, Gundavelli teaches wherein said determining uses only said first key and said second key (column 5, lines 47-63, column 11, lines 6-39).

20.   Regarding claims 20 and 21, Gundavelli teaches wherein said subgroup includes only said first user or a plurality of users (column 5, lines 47-63, column 11, lines 6-39).

21.   Claims 28-30 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,240,188 to Dondeti et al., hereinafter Dondeti.

22.   As per claim 28, Dondeti teaches a keying method in an environment having a plurality of users, each user being capable of storing a set of keys that enable secure communication among sets of said plurality of users, comprising:

(a) distributing first information that enables users to update, after eviction of one or

more users, a set of compromised keys that are known to said one or more users without

receiving new key information (column 8, line 43 to column 9, line 19).

23.   Regarding claim 29, Dondeti discloses wherein said first information includes

information that enables identification of a one-way function (column 3, line 64 to column 4, line

21).

24.   Regarding claim 30, Dondeti teaches wherein said first information includes information

that enables identification of said evicted one or more users (column 8, line 43 to column 9, line

19).

25.   Claims 38 and 39 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent

No. 6,295,361 to Kadansky et al., hereinafter Kadansky.

26.   As per claims 38 and 39, Kadansky discloses a secret sharing system, comprising:

        a key server that distributes secret information to a plurality of users, wherein each user is

sent secrets that are shared by respective sets of said plurality of users, said key server being

operative to update at least one compromised secret known by at least one evicted user at least

one non-compromised secret that is not known by said at least one evicted user (column 1, line

66 to column 2, line 61).

Claim Rejections - 35 USC § 103

27.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

28.   Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gundavelli in view

of U.S. Patent No. 6,178,244 to Takeda, hereinafter Takeda.

29.   With regards to claim 7, Gundavelli does not teach wherein said updating occurs on a

periodic basis.

30.   Takeda teaches wherein said updating occurs on a periodic basis (column 12, lines 38-

43).

31.   Both Gundavelli and Takeda both disclose updating keys for group communication.

32.   It would have been obvious to one of ordinary skill in the art at the time the invention

was made to update the keys on a periodic basis, since Gundavelli states at column 7, lines 25-

38, that the communication occurs over the Internet and therefore may be subject to sniffing, or

the spying of packets. Therefore, one of ordinary skill would recognize that changing the key

periodically would make it more difficult for an eavesdropper to intercept group

communications.

33.   Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Gundavelli in view Dondeti.

34.   With regards to claim 17, Gundavelli does not disclose wherein said determining uses a

one-way function.

35.   Dondeti teaches wherein said determining uses a one-way function (column 3, line 64 to

column 4, line 21).

36.   It would have been obvious to one of ordinary skill in the art at the time the invention

was made to determine the new key using a one-way function, since Dondeti states at column 4,

lines 7-21 that such a modification would make it computationally infeasible to compute the key.

37.   Concerning claim 18, Gundavelli teaches wherein said updated first key is equal to F(first

key, second key) (column 5, lines 47-63, column 11, lines 6-39).

38.   Gundavelli does not teach wherein F() is a one-way function.

39.   Dondeti teaches wherein F() is a one-way function (column 3, line 64 to column 4, line

21).

40.   It would have been obvious to one of ordinary skill in the art at the time the invention

was made to determine the new key using a one-way function, since Dondeti states at column 4,

lines 7-21 that such a modification would make it computationally infeasible to compute the key.

Conclusion

41.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

42.   The following patents are cited to further show the state of the art with respect to re-

keying, such as:

United States Patent No. 6,901,510 to Srivastava, which is cited to show distributing and updating group controllers over a wide area network using a tree structure.

United States Patent No. 6,330,671 to Aziz, which is cited to show secure distribution of cryptographic keys on multicast networks.

United States Patent No. 5,630,184 to Roper et al., which is cited to show deleting and adding nodes in a spanning tree network by collating replies from other nodes.

United States Patent No. 6,151,395 to Harkins, which is cited to show regenerating secret keys in Diffie-Hellman communication sessions.

United States Patent No. 6,483,921 to Harkins, which is cited to show regenerating secret keys in Diffie-Hellman communication sessions.

43.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

44.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

45.   Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100